CFRG Working Group
Internet Draft
Intended status: Experimental

P. Urien
Telecom ParisTech

February 7 2015

Expires: August 2015

Cloud of Secure Elements(CoSE)
draft-urien-cfrg-cose-02.txt

Abstract

This document describes an architecture named "Cloud of Secure Elements (CoSE)" whose goal is to strengthen the Internet trust. A Secure element (SE) provides secure services thanks to various means such as tamper resistant technologies or software virtualization techniques. Secure elements are hosted in dedicated servers (i.e. Trusted Secure Elements Servers, TSES); they provide secure storage facilities or compute cryptographic procedures. Secure elements resources are identified by dedicated URIs and should also support HTTP interface. Users are equipped with "Access Credential" and thanks to the Secure Transport Protocol (STP-TSES) remotely access to Secure Element embedded resources. The RACS (Remote APDU Call Secure) and its associated framework protocol is an early proof of concept of the CoSE concept.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 2015.

Copyright Notice

Table of Contents

Abstract 1
Requirements Language 1
Status of this Memo 1
Copyright Notice 2
1 Overview 4
2. Architecture 5
2.1 Trusted Secure Element Servers (TSES) 5
2.2 Secure Transport Protocol (STP-TSES) 6
2.3 Users and Administrators 6
3. Remote APDU Call Secure (RACS) 7
4 Security Considerations 7
5 IANA Considerations 7
6 References 8
6.1 Normative References 8
6.2 Informative References 8
7 Authors' Addresses 8

1 Overview

Internet technologies are more and more pervasive. Connected users and devices produce and consume data that are exchanged over the network and stored in data centers. The IETF has defined multiple standards providing secure features such as authentication, privacy or data integrity.

However the Internet suffers from a lack of trust. Recent facts were reported by the press about pervasive surveillance over Internet users; even if Internet protocols support privacy features, these procedures require secret keys and strong cryptographic algorithms.

There is a trust issue towards all entities that provide cryptographic facilities and secure storage of sensitive data. It makes may wonder how trust these services are; in other words who may access to secret values storage and use?.

In this document we discuss an architecture draft, named "Cloud of Secure Elements (CoSe)", whose goal is to strengthen the Internet trust.

Trust is a complex concept. A banknote is the root of trust for commercial exchanges in a set of countries. Trust relies on national, cultural, educative, social or professional beliefs. For the most part, Internet trust relies on secure storage of passwords both on users and servers sides.

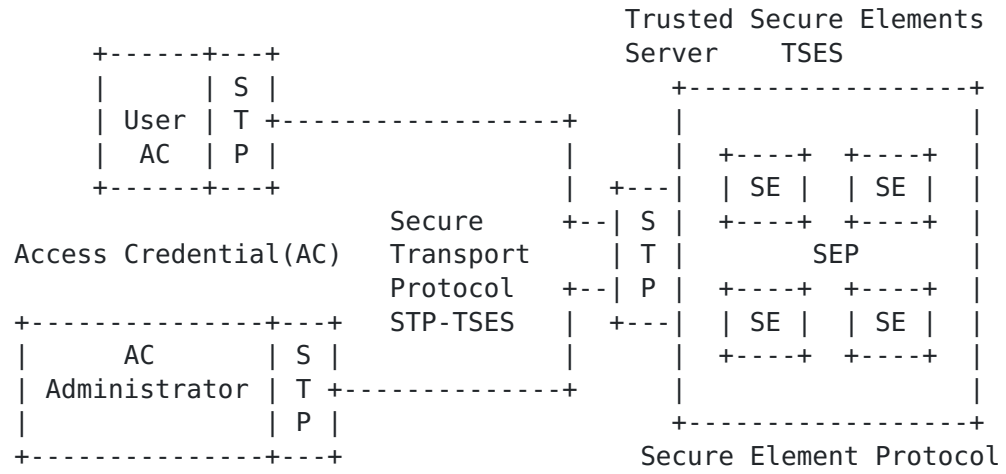
The basic idea of the proposed architecture is to deploy Trusted Secure Element Servers (TSES), whose trusted internal components (the secure elements) could be used and managed by human or software entities. This functional granularity is a key feature for the CoSE paradigm.

TSES servers are managed by a plurality of entities and realized security services for isolated users or numerous users. They could be fitted for individual or worldwide needs.

TSES servers are accessed thanks to a Secure Transport Protocol (STP-TSES), which always works with a strong mutual authentication, which is used both for service and administration purposes, and which is interoperable with all TSES.

Users or administrators are connected to TSES servers thanks to the STP-TSES protocol. They need Access Credentials (AC) for mutual authentication with TSES. Cryptographic procedures, long term secrets, sensitive data are executed or stored in TSES. Users work with multiple terminals with different level of trust and security. These devices remotely access to critical data and procedures thanks their Access Credentials; this feature implies native traceability and easy revocation for lost or compromise terminals.

2. Architecture



The Cloud of Secure Elements comprises the following components:
- A set of Trusted Secure Element Servers (TSES).
- Secure Transport Protocol (STP-TSES), working with all TSES.
- Users and administrators, implementing STP-TSES, and equipped with Access Credentials (AC).

2.1 Trusted Secure Element Servers (TSES)

A Trusted Security Server manages a set of trusted entities called Secure Elements (SE). A secure element provides secure services thanks to various means such as tamper resistant technologies or software virtualization techniques.

The main hypothesis is that users trust the SEs hosted in the TSES.

Secure Elements realizes services such as secure storage or cryptographic procedures. These services are remotely installed, updated or deleted by management entities.

Therefore SEs work according to two functional planes,
- An administrative plane.
- A user plane.

According to the CoSE model, the SE MUST provide isolated and safe computing environment, according to criteria (for example certifications) that are trusted by the users. SEs entities are accessed via physical or logical protocols referred as Secure Element Protocol (SEP).

There are two classes of SEP:
- Protocols (SEP-BER) based on well-known binary encoding rules (BER), for example ISO7816 commands [ISO7816] exchanged with secure ISO7816 microcontrollers.

- Protocols (SEP-API) based on the transport of application programming Interface (API), for example the PKCS#11 [PKCS#11] API usually referred as "cryptoki" widely used for the interface of hardware secure module (HSM).

2.2 Secure Transport Protocol (STP-TSES)

The Secure Transport Protocol (STP-TSES) drives the data exchange between users and TSES servers. It MUST enforce a strong mutual authentication between these entities, and also support identity protection features on the client side.

The STP-TSES creates a secure session with the TSES server.

The STP-TSES mainly provides two services:
- The inventory of SEs hosted in TSES servers
- The transport of SEP messages, and their routing towards the targeted Secure Element.

Each SE is identified by a secure element identifier (SEID).

STP-TSES services SHOULD be compatible with the [REST] (Representational State Transfer) architecture.

Secure elements resources SHOULD be identified by dedicated URIs (Uniform Resource Identifier).

An HTTP interface SHOULD be also supported.

2.3 Users and Administrators

Users and administrators drive the data exchanges with TSES via the STP-TSES protocol. There are equipped with Access Credentials (AC) needed for mutual authentication with the TSES.

A secure tunnel is opened with the TSES. Thanks to their ACs attributes, users and administrators privileges, dealing with the two functional planes (user and administrative), are established by the TSES.

Because Secure Elements handle cryptographic facilities, a second secure channel MAY be opened between users (or administrators) and SEs.

3. Remote APDU Call Secure (RACS)

RACS stands for "Remote APDU Call Secure" [RACS]. It is an early proof of concept of the Cloud of Secure Elements.

The RACS framework enables secure remote access of data and cryptographic procedures hosted in the CoSE. These elements are identified by URIs and also support an HTTP interface.

In the RACS context, a Secure Element (SE) is a tamper resistant microcontroller equipped with host interfaces such as ISO7816, SPI (Serial Peripheral Interface) or I2C (Inter Integrated Circuit).

The typical area size of these electronic chips is about 25mm2. They comprise CPU (8, 16, 32 bits), ROM (a few hundred KB), nonvolatile memory (EEPROM, FLASH, a few hundred KB) and RAM (a few ten KB). Security is enforced by multiple hardware and logical countermeasures.

These Secure Elements are hosted in servers, whose commercial appliances are usually referred as SIM-Servers.

The RACS protocol, is transported over the TLS protocol [TLS 1.0] [TLS 1.1] [TLS 1.2], and works with a mandatory mutual authentication. Both server and client are equipped with certificates and associated private keys. RACS is used for the transport of SEP messages; it also supports features for the SEs inventory.

The SE protocol is based on the ISO7816 protocol, which defines the binary encoding rules for request and response packets exchanged with SE, refereed as APDUs (Application Protocol Data Unit).

The administration is compliant with a set of Global Platform [GP] standards, which controls the lifecycle of SE embedded software, i.e. application downloading, activation and deletion.

4 Security Considerations

To be done.

5 IANA Considerations

To be done.

6 References

6.1 Normative References

[TLS 1.0] Dierks, T., C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999

[TLS 1.1] Dierks, T., Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006

[TLS 1.2] Dierks, T., Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.1", draft-ietf-tls-rfc4346-bis-10.txt, March 2008

[ISO7816] ISO 7816, "Cards Identification - Integrated Circuit Cards with Contacts", The International Organization for Standardization (ISO)

6.2 Informative References

[PKCS#11] PKCS#11, "Cryptographic Token Interface Standard", RSA Laboratories.

[REST] Fielding, R., "Architectural Styles and the Design of Network-based Software Architectures", 2000, http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

[GP] Global Platform Standards, http://www.globalplatform.org

[RACS] Remote APDU Call Secure (RACS), draft-urien-core-racs-00.txt

7 Authors' Addresses

Pascal Urien
Telecom ParisTech
23 avenue d'Italie
75013 Paris Phone: NA
France Email: Pascal.Urien@telecom-paristech.fr